UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/524,573	02/15/2005	Declan Patrick Kelly	NL 020775	8318

24737 7590 05/23/2008
PHILIPS INTELLECTUAL PROPERTY & STANDARDS
P.O. BOX 3001
BRIARCLIFF MANOR, NY 10510

EXAMINER	
YOUSEFI, SHAHROUZ	

ART UNIT	PAPER NUMBER
2132	

MAIL DATE	DELIVERY MODE
05/23/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/524,573	KELLY, DECLAN PATRICK	
	Examiner	Art Unit	
	SHAHROUZ YOUSEFI	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 August 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-15* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-15* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *15 February 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *08-10-2005*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claim15 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Data structures not claimed as embodied in computer-readable media are descriptive material per se and are not statutory because they are not capable of causing functional change in the computer. See MPEP 2106.01 and e.g., Warmerdam, 33 F.3d at 1361, 31 USPQ2d at 1760.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim 1 is rejected under 35 U.S.C. 103(a) as being unpatentable over Arcot Desal et al. (EP 0 644 474 A1) in view of Quick, Jr. et al. (US 2002/0091931).

With respect to claim 1, Arcot Desal et al. teaches that A method of protecting content stored on a storage medium against unauthorised access, said storage medium being accessible by a drive (D) of a portable device which is connectable to a network (1), comprising the steps of: (a method for preventing unauthorized copying and use of

information which is stored on a storage medium, abstract) transmitting an identifier (id) of said storage medium or the user to an authentication unit (Auc) within said portable device or within said network (the device ID (DID-S) stored in the distribution medium, abstract), generating a cryptographic key (ck) using said identifier (id) and an authentication key (ak) by an authentication algorithm within said authentication unit (Auc) (generating a key from both the signature of the distribution medium and the DID-S, page 2, line 58). However, Desal et al. doesn't teach transmitting of cryptographic key from authentication unit. But Quick, JR. et al. teaches that transmitting said cryptographic key (ck) from said authentication unit (Auc) to said drive (D), encrypting the content to be protected using said cryptographic key (ck), and storing the encrypted content on said storage medium (Both the Secure Key 300 and the random number 240 are used by a key generator 250 to generate the confirmation message 260, a cryptographic Cipher Key (CK) 290, and an Integrity Key (IK) 310. The CK 290 and IK 310 are conveyed to the mobile unit 220, par. [0025]). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to modify the storage medium of Arcot Desal et al. with cryptographic key (ck) of Quick, JR. et al. which is used for encryption or an authentication key for identifying the subscriber to mobile phone, to prevent unauthorized copying and use of information which is stored on a storage medium and restrict the use of such information to designated devices.

With respect to claim 2, Arcot Desal et al. teaches that said identifier (id) is stored on said storage medium in machine-readable form and is read before transmission to said authentication unit (Auc) (the personal computer ID is used with the source ID on

the distribution diskette to produce an encoded check word, using any available encryption method, page1, lines 33-34).

With respect to claim 3, Arcot Desal et al. teaches that said authentication unit is part of said portable device (Next, the ID of the designated device is authenticated in step 200 by the device veri- fication program DVP, page 5, line 55).

With respect to claim 4, Quick JR. et al. teaches that said authentication key (ak) is stored within said authentication unit or on a removable authentication memory, in particular a SIM card, which is readable by said authentication unit (transmit the private information to another storage unit during the legitimate use of the mobile phone, par. [0007]).

With respect to claim 5, Quick JR. et al. teaches that said authentication unit (Auc) is part of said network (a wireless communication network 10 generally includes a plurality of mobile stations, par. [0017]).

With respect to claim 6, Arcot Desal et al. teaches that said storage medium is a removable record carrier, such as an optical disk, a removable hard disk or a semiconductor memory card (by storage medium, the present invention refers to all types of non-volatile storage medium, page 2, lines 13-14).

With respect to claim 7, Arcot Desal et al. teaches that said storage medium is a non-removable storage medium, such as a semiconductor memory or a non-removable hard disk (by storage medium, the present invention refers to all types of non-volatile storage medium, page 2, lines 13-14).

With respect to claim 8, Quick JR. et al. teaches that said portable device is a mobile phone, wherein said authentication unit is a SIM card reader, wherein said network is a mobile phone network and wherein said authentication algorithm corresponds to the algorithm used by said mobile phone network for authenticating mobile phones (A subscriber identification token 230 provides authentication support by generating a signature 370 based upon a key that is held secret from a mobile unit 220, abstract).

With respect to claim 9, Arcot Desal et al. teaches that said identifier (id) is the PIN of the user (the device ID (DID-D) of the device with the device ID (DID-S) stored in the distribution medium, abstract) the identifier in this case is device id and it could be the device PIN in case of this the invention, the identifier is a specific number which identify particular mobile device for plurality of devices.

With respect to claim 10, Quick JR. et al. teaches that said identifier (id) is transmitted from said portable device to said authentication unit (Auc) via the internet and a link from the internet to said network, in particular via a computer connected to the internet (FIG. 1, a wireless communication network 10 generally includes a plurality of mobile stations (also called subscriber units or user equipment) 12a-12d,...or internetworking function (IWF) 20, a public switched telephone network (PSTN) 22 (typically a telephone company), and an Internet Protocol (IP) network 18 (typically the Internet), par. [0017]).

With respect to claim 11, Arcot Desal et al. teaches that means for connecting said device to a network, a drive (D) for accessing said storage medium, in particular for

reading content from and writing content to said storage medium, a transmitter for transmitting an identifier (id) of said storage medium or the user to an authentication unit (Auc) within said device or within said network (the device ID (DID-S) stored in the distribution medium, abstract), a receiver for receiving a cryptographic key (ck) generated within said authentication unit (Auc) by an authentication algorithm using said identifier (id) and an authentication key (ak) and for transmitting said cryptographic key (ck) to said drive (D) (generating a key from both the signature of the distribution medium and the DID-S, page 2, line 58), However, Desal et al. doesn't teach encryption means. But Quick, JR. et al. teaches that encryption means (D) for encrypting content to be protected using said cryptographic key (ck) for storage on said storage medium (these techniques can take the form of encryption techniques, hashing functions, or any nonreversible operation. par. [0037]). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to modify the encryption method of Quick, JR. et al. with storage medium of Arcot Desal et al. to secure the digital information on one storage medium.

With respect to claim 12, Arcot Desal et al. teaches that transmitting an identifier (id) of said storage medium or the user to an authentication unit (Auc) within said portable device or within said network (the device ID (DID-S) stored in the distribution medium, abstract), generating a cryptographic key (ck) using said identifier (id) and an authentication key (ak) by an authentication algorithm within said authentication unit (Auc) (generating a key from both the signature of the distribution medium and the DID-S, page 2, line 58), transmitting said cryptographic key (ck) from said authentication unit

(Auc) to said drive (D), and decrypting the content to be accessed using said cryptographic key (ck) (Decryption of the information is accomplished by generating a key from both the signature of the distribution medium and the DID-S, page 2, lines 57-58).

With respect to claim 13, Arcot Desal et al. teaches that means for connecting said device to a network, a drive (D) for accessing said storage medium, in particular for reading content from and writing content to said storage medium (a method for preventing unauthorized copying and use of information which is stored on a storage medium, abstract), a transmitter for transmitting an identifier (id) of said storage medium or the user to an authentication unit (Auc) within said device or within said network (the device ID (DID-S) stored in the distribution medium, abstract), a receiver for receiving a cryptographic key (ck) generated within said authentication unit (Auc) by an authentication algorithm using said identifier (id) and an authentication key (ck) and for transmitting said cryptographic key (ck) to said drive (D), and decryption means (D) for decrypting content to be accessed using said cryptographic key (ck) (Decryption of the information is accomplished by generating a key from both the signature of the distribution medium and the DID-S, page 2, lines 57-58).

With respect to claim 14, Quick et al. teaches that said device is a mobile phone, wherein said authentication unit is a SIM card reader, wherein said network is a mobile phone network and wherein said authentication algorithm corresponds to the algorithm used by said mobile phone network for authenticating mobile phones (A subscriber

identification token 230 provides authentication support by generating a signature 370 based upon a key that is held secret from a mobile unit 220, abstract).

With respect to claim 15, Arcot Desal et al. teaches that computer program code means for causing a computer to perform the steps of the method as claimed in claim 1 when said program is run on a computer. Claim 15 provides all limitations of claim 1 and is rejected based on the same grounds as claim 1 rejection.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SHAHROUZ YOUSEFI whose telephone number is (571) 270-3558. The examiner can normally be reached on Monday-Thursday 9:00-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 5712723799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Shahrouz Yousefi/
Examiner, Art Unit 2132
03/20/2008

/Gilberto Barron Jr/
Supervisory Patent Examiner, Art Unit 2132